ASA VPN-clientverbinding via een L2L-tunnelconfiguratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco adaptieve security applicatie (ASA) moet configureren om een externe VPN-clientverbinding mogelijk te maken vanaf een LAN-to-LAN (L2L) peer-adres.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ASA
- Remote Access VPN's
- LAN-to-LAN VPN's

Gebruikte componenten

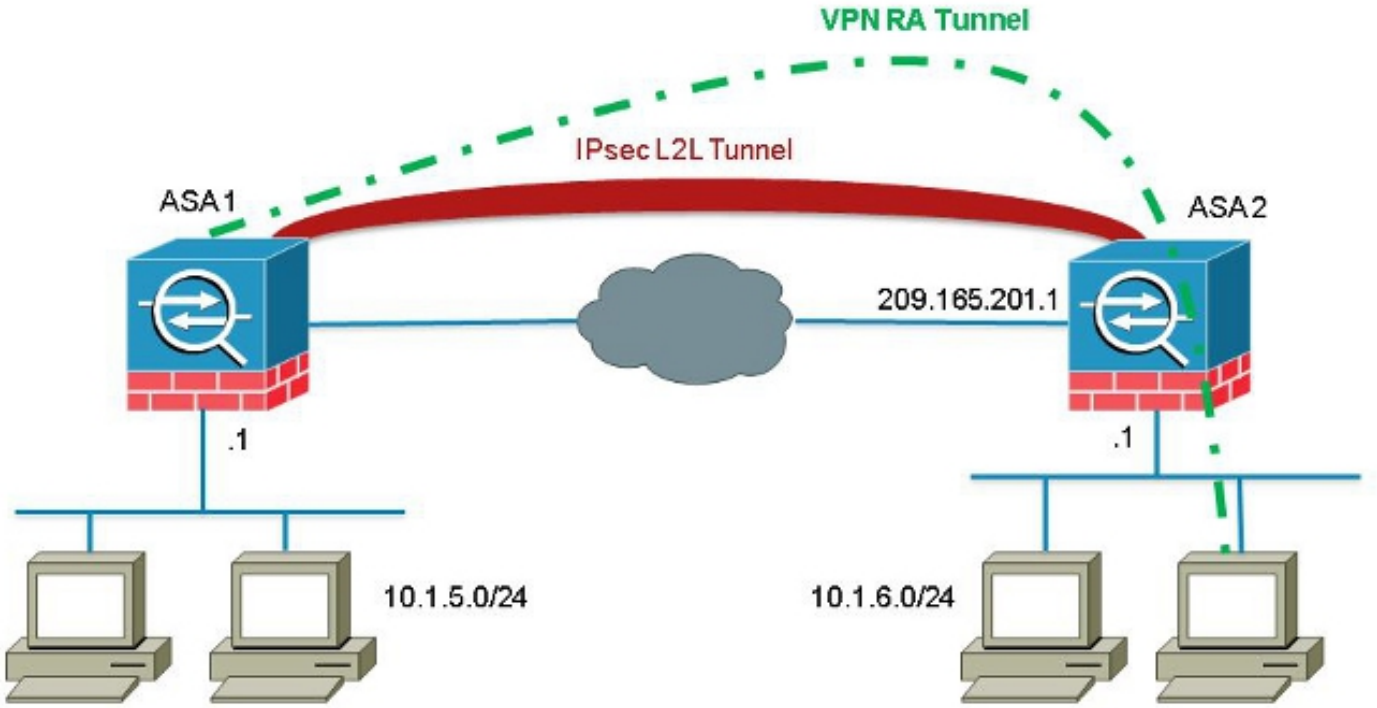
De informatie in dit document is gebaseerd op Cisco 5520 Series ASA die software versie 8.4(7) draait.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Hoewel het niet gebruikelijk is om een scenario te ervaren waar een VPN-client probeert een verbinding tot stand te brengen via een L2L-tunnel, zouden beheerders specifieke voorrechten of toegangsbeperkingen aan bepaalde externe gebruikers willen toewijzen en hen kunnen opdragen de softwareclient te gebruiken wanneer toegang tot deze bronnen vereist is.

> Opmerking: Dit scenario werkte in het verleden, maar na een upgrade van de head-end ASA naar versie 8.4(6) of later kan de VPN-client de verbinding niet langer opzetten.



Cisco bug ID CSCuc75090 heeft een gedragsverandering geïntroduceerd. Eerder, met de Private Internet Exchange (PIX), toen de IPSec-proxy (Internet Protocol Security) geen crypto-map Access Control List (ACL's) had, bleef deze security in de lijst staan. Dit omvatte overeenkomsten met een dynamische crypto-kaart zonder peer gespecificeerd.

Dit werd gezien als een kwetsbaarheid, omdat afstandsbeheerders toegang konden krijgen tot middelen die de head-end beheerder niet van plan was toen de statische L2L werd geconfigureerd.

Er werd een oplossing gemaakt die een check toevoegde om lucifers met een crypto-kaart ingang zonder een peer te voorkomen toen het al een map ingecheckt die het peer vond. Dit had echter gevolgen voor het scenario dat in dit document wordt besproken. Met name is een externe VPN-client die probeert verbinding te maken met een L2L-peer-adres niet in staat verbinding te maken met het head-end.

Configureren

Gebruik deze sectie om de ASA te configureren om een externe VPN-clientverbinding toe te staan

vanaf een L2L peer-adres.

Voeg een nieuw Dynamisch Begin toe

Om externe VPN-verbindingen van L2L peer-adressen toe te staan, moet u een nieuwe dynamische ingang toevoegen die hetzelfde IP-adres bevat.

> Opmerking: U moet ook een andere dynamische ingang zonder peer verlaten zodat elke cliënt van het internet ook kan verbinden.

Hier is een voorbeeld van de vorige dynamische crypto-kaart werkconfiguratie:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Hier is de dynamische crypto-kaart configuratie met de nieuwe dynamische ingangsconfiguratie:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.